REMARKS

The Office Action of September 14, 2006 has been received and carefully considered. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the following comments.

REJECTIONS UNDER 35 U.S.C. § 102:

Claims 1, 3 and 5 have been rejected under 35 U.S.C. § 102 (b) as allegedly being anticipated by Schneier (Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons).

According to MPEP 2131, "A claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). In the Office Action, the Examiner indicated that Schneier discloses key bit permutation operation depending on the converted data. In addition, since Schneier does not describe such operation, because it is not used in DES algorithm, the Examiner has established connection between a fixed permutation performed on a key to form the predetermined encryption round and the data block which is converted at the predetermined encryption round.

Applicant respectfully disagrees with such interpretation of DES encryption algorithm that is well known to a person of ordinary skill in the art. Connection arbitrarily established by the Examiner between the round key, e.g., for the I-th round, and the subblock value at the I-th round has a general philosophical sense. But it does not relate to the technical content of the conversion procedures and operations used in DES algorithm as understood by a person of ordinary skill in the art. In a general philosophical sense, forming a DES algorithm round key used in DES algorithm in the I-th round depends on the data block converted in AES encryption algorithm, which is a new

encryption standard and which not known when DES algorithm was developed. From positions of technical consideration, such conclusion is not supported by the facts.

The fact that, in DES algorithm, round keys are formed regardless of data converted, is supported by the following obvious facts:

1. Independently of data converted, at each predetermined encryption round, the dame round key is used.
2. All round keys can be calculated in advance, i.e. before the point when a data block for encryption will be selected using DES algorithm.

These facts are supported by well-known literature references describing DES algorithm. These references describe the procedure of forming DES round keys as an independent one and not depending on data converted.

Applicant respectfully submits that the explanations to the description of DES in Schneier, which Applicant set forth in the previous response to the previous Office Action, are corrected and correspond to the technical content of DES algorithm. These explanations clearly disclose the technical essence of all DES algorithm procedures which are correctly described in Schneier and in a great number of other documents and do not include the key bit permutation operation performed depending on the data converted. A person of ordinary skill in the art who is familiar with block encryption methods can confirm this position.

Applicant, once again, respectfully quotes the following passage from the pervious response: on page 272, in section "The Key Transformation", Schneier discloses what bit permutation operation was performed on the subkey: "First, the 56-bit key is divided into two 28-bit halves; Then, the halves are circulated shifted left by either one or two bits, depending on the round." Thus, in algorithm DES, the bit permutation operation is performed on the key depending on the number of the round and not on the data subblock, i.e. the feature of performing the subkey bit permutation operation depending on the data subblock being converted, that is present in the claimed invention, is novel.

Therefore, the currently presented claims are not anticipated by Schneier and the rejection under 35 U.S.C. § 102 (b) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (b) is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: January 5, 2007
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0

By _____
John C. Holman
Registration No. 22,769